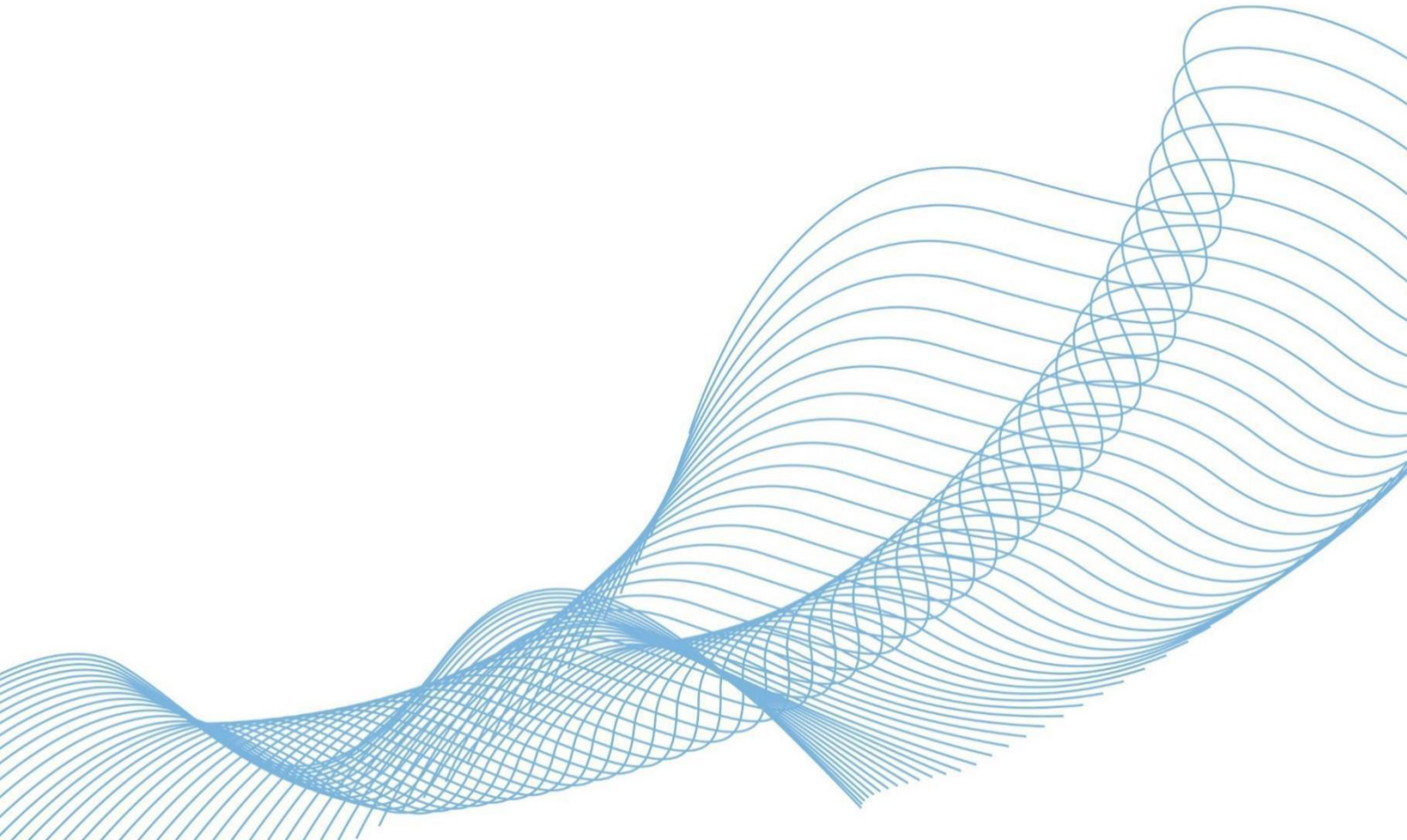
联软科技
LEAGSOFT

Endpoint Detection and Response (EDR) System Technical White Paper



Contents

1. Statement

1.1 Disclaimer

The products, services, or features you purchase are subject to the terms and conditions of the commercial agreement between you and Shenzhen Leagsoft Technology Co., Ltd. The products, services, or features described in this document may not be included within the scope of your purchase or usage. Unless otherwise specified in the contract, Shenzhen Leagsoft Technology Co., Ltd. does not make any explicit or implicit statements or guarantees about the content of this document.

Due to product version upgrades or other reasons, the content of this document may be updated periodically. Unless otherwise specified, this document serves as a reference guide for use only, and all information, recommendations, and exclusions in this document are not intended to constitute any explicit or implied warranty.

1.2 Contact Us

Service Center Email: support@leagsoft.com.

Technical Support Hotline: 400-6288-116

Official Website: http://www.leagsoft.com

2. Preface

2.1 Security Background and Challenges

Currently, information technology is impacting various industries, with digital transformation and upgrading trends becoming increasingly evident across all sectors. Information security has also become a primary focus for many industries. As IT technology advances, hacker attack techniques are evolving in response. The "2019 Cost of a Data Breach Report" released by IBM Security indicates that "the number of data breaches increased by 52% compared to 2018, with costs rising by 12% over five

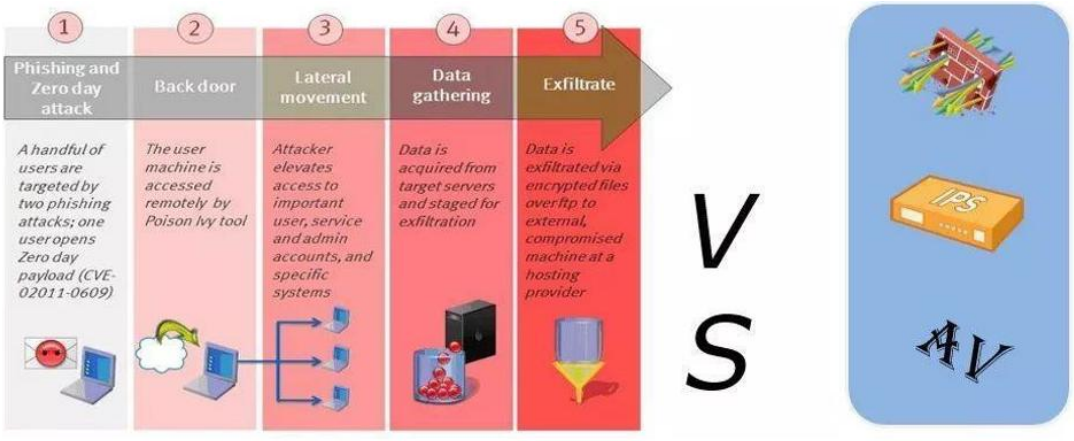
years to reach $3.92 million." Similarly, the "2019 Global Advanced Persistent Threat (APT) Research Report" by Tencent Yujian Threat Intelligence Center shows that in 2019, global security vendors disclosed nearly 500 APT attack reports, reflecting an approximate 10% increase compared to 2018.

While companies are increasing investments in information security construction, and various security systems are gradually being deployed, 80% of these systems still fail to guard against 80% of the risks. Endpoints, as the primary devices used by corporate employees, have become the main battlefield for hacker attacks. However, traditional endpoint protection solutions are increasingly unable to counter current attack methods. The main issues are as follows:

Traditional endpoint protection solutions struggle to combat sophisticated and targeted attacks.
Previous endpoint protection solutions focused primarily on defense, driven by policies, signatures, and internal regulations. However, attackers can easily bypass these defenses using customized malware or targeted attack techniques, directly threatening internal security.

Traditional endpoint protection solutions lack attack traceability.
Existing endpoint security solutions detect and alert based on specific policies or signatures but lack continuous monitoring of endpoints. Once a threat occurs, administrators cannot trace the incident, making it challenging to identify the source and assess the impact of the threat.

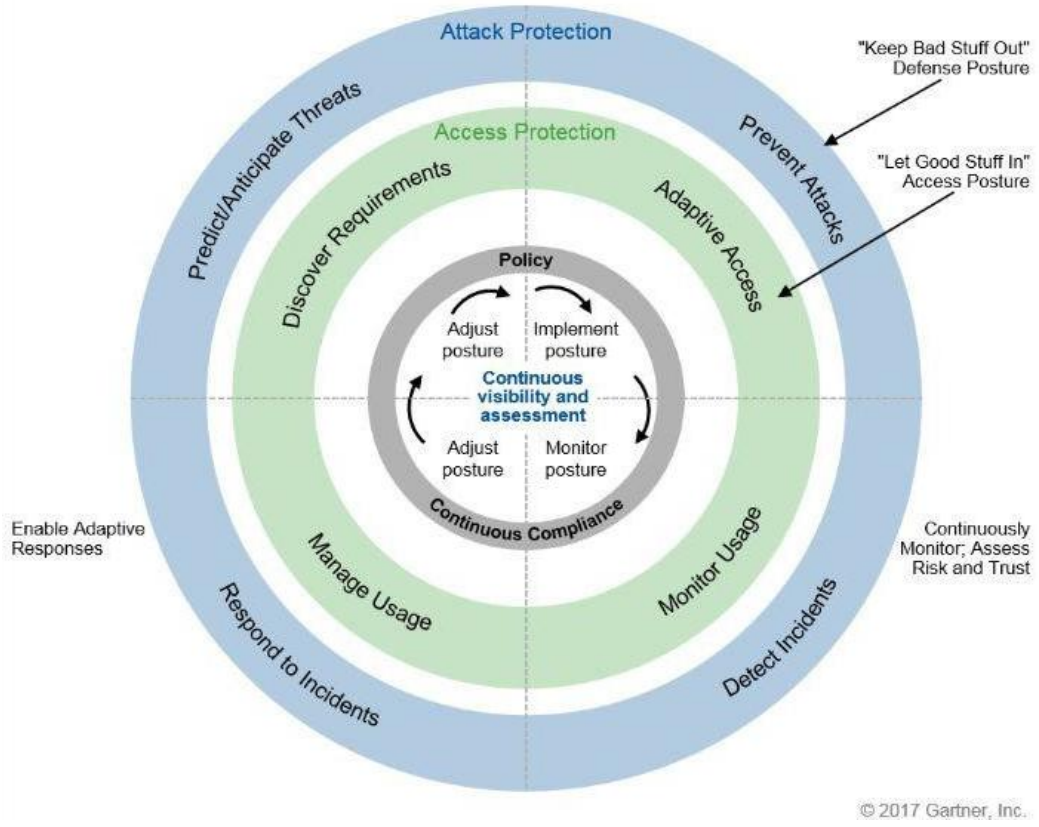
Traditional endpoint protection solutions have lengthy incident response times.
Current endpoint protection systems often operate independently without effective correlation between alerts, making it difficult for administrators to gain a comprehensive view of security incidents. As a result, they may become overwhelmed by excessive alert filtering and unable to respond and address threats promptly, further exacerbating the impact of the threat.



Advanced Persistent Threat (APT)

Signature-Based Traditional Defense

Based on these challenges, Gartner introduced the concept of ETDR in 2013 and formally named it EDR (Endpoint Detection and Response) in 2015. EDR is defined as a "solution that records and stores endpoint system-level behaviors, uses various data analysis techniques to detect suspicious system behaviors, provides contextual information, blocks malicious activities, and offers remediation recommendations to restore affected systems." The primary functions include detecting security incidents, investigating security incidents, containing security incidents on endpoints, and restoring endpoints to their pre-infection state.



CARTA's "Continuous Adaptive Risk and Trust" Security Model

3. Product Overview

Leagsoft Endpoint Detection and Response (EDR) System is a security management platform developed by Leagsoft Technology based on Gartner's EDR concept and the Continuous Adaptive Risk and Trust Assessment (CARTA) security model. It is designed to address advanced endpoint threats, trace attacks, and assist enterprises in continuous improvement of endpoint security control. Products can be expanded through the existing Leagsoft Endpoint Protection Platform (EPP), allowing for

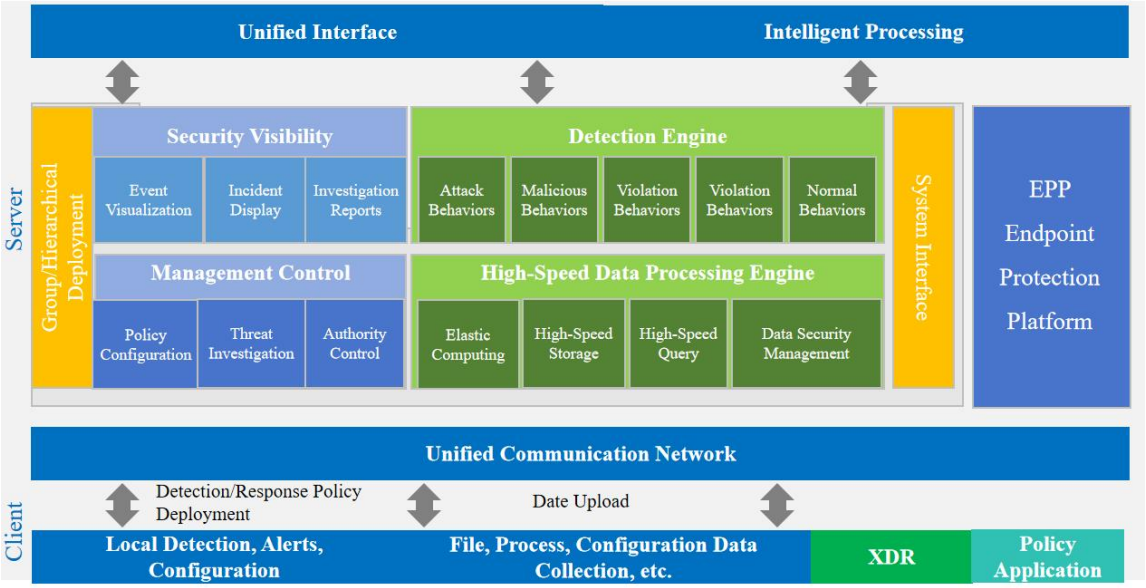
unified customer management on a single platform. This approach enables achieve complementary security capabilities, where the UniEDR system detects, handles, and analyzes threats. The Leagsoft EPP platform then leverages threat traceability and analysis results to continuously improve endpoint security management configurations, fostering a trend of ongoing enhancement in internal endpoint security for enterprises.

4. Product Architecture

4.1 Architecture Design

The Leagsoft Endpoint Detection and Response (EDR) System consists of two main components: the client side and the server side.

The client side is deployed on user endpoints through an agent, which is responsible for data collection and threat handling. The server side comprises three main parts: the data processing engine, detection engine, and management platform.



Client Side:

The client side consists of the agent and security components deployed on endpoints. Its main functions include monitoring the operating system behavior of endpoints, accurately identifying known threats, making preliminary judgments and alerts on unknown threats, capturing and reporting threats, and executing operations such as alerting, blocking, intercepting, and removing various threats. It can also perform multiple handling tasks issued by the management center.

The client supports the collection of all data related to security behaviors on the

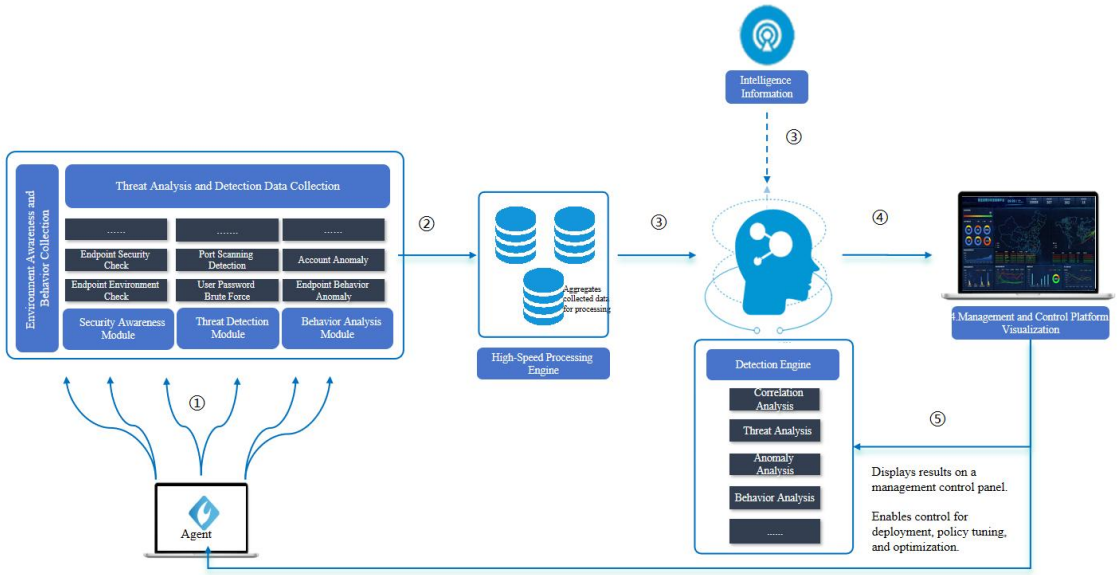
endpoint, including Basic Information, such as host information, system user information, system service information, and PE (Portable Executable) information. Endpoint Event Logs: covering events like process start, process exit, process injection, file operations, network access, DNS access, operating system user logins, operating system logs, and PowerShell execution events. Endpoint Change Records: including changes to the registry, auto-start programs, system users, services, and drivers.

High-Speed Data Processing Engine:
Primarily used for storing terminal security data information submitted by client endpoints, this engine enables rapid processing and efficient retrieval of all terminal security information. Traditional relational databases often face performance limitations when handling large volumes of data, resulting in slow data query responses. To address this, Leagsoft developed its proprietary high-speed data processing engine, AcutaDB, as a dedicated solution for fast data storage and processing on the server side. AcutaDB achieves data access speeds over ten times faster than traditional databases and supports multi-device clustering to ensure ample storage capacity and computational power.

Detection Engine:
Primarily used to analyze security data submitted by client endpoints, this engine abstracts and generalizes normal behavior patterns of endpoints. Utilizing machine learning and big data correlation analysis, it generates behavior profiles for each endpoint. Based on these profiles, the engine then assesses whether endpoint behavior deviates from normal patterns, detects anomalies, and determines if any threats may be present. This process aids security personnel in identifying potential risks promptly.

Management Console:
Primarily designed for security management personnel, the management console enables unified security management of endpoint assets. It centralizes monitoring and analysis of endpoint security incidents, formulates and deploys relevant response task strategies, and provides threat tracking and alert response capabilities. The threat tracking feature allows operations personnel to manually search endpoint security data across the entire network, supporting both fuzzy and precise search to locate valuable specific content quickly. It also enables filtering, categorizing, and statistical analysis of specific data types, making it easier for experienced security operations personnel to proactively identify internal network security incidents and execute security response actions.

4.2 Endpoint Security Protection Closed-Loop Process



5. Product Features

5.1 Data Collection Technology Based on Multiple Dimensions

Unlike traditional endpoint security management systems that rely on signatures, the Endpoint Detection and Response (EDR) system is based on automated data analysis to infer high-probability harmful attack behaviors. The system collects fundamental data from endpoints through the client, converts this data into behavioral operations, analyzes these operations to identify potential attack behaviors, and recognizes those that pose a threat to enterprise information security.

As the first step in the EDR process, fundamental data serves as the basis for threat detection capabilities. Inaccurate or missing fundamental data can lead to numerous false judgments and omissions.

Leagsoft's EDR supports the collection of all security-related data on endpoints, including:

Basic Information: host information, system user information, system service information, and PE (Portable Executable) information.

Endpoint Event Logs: process start events, process exit events, process

injection events, file operation events, network access events, DNS access events, operating system user login events, OS log events, and PowerShell execution events.

Endpoint Change Logs: registry changes, auto-startup changes, system user changes, service changes, and driver changes.

This comprehensive data collection enables a robust foundation for detecting and responding to threats.

5.2 Endpoint Threat Behavior Detection

By applying deep learning, reinforcement learning, correlation analysis, and clustering analysis to all security-related data on endpoints, the system proactively uncovers and identifies hidden security threats on endpoints. Additionally, monitoring indicators can be set based on the client's business operations to establish a multi-dimensional, multi-layered, in-depth detection system for file processes, host access, business relationships, and more. This enables continuous monitoring of intrusion activities, achieving real-time intrusion detection. Once any abnormal activity is detected, the system triggers an alert within milliseconds.

5.3 Terminal Threat Defense

Leagsoft EDR enables comprehensive network-wide tracing of malicious files/processes detected on individual endpoints within an enterprise's intranet. Through custom global searches or YARA and Braise syntax, the system conducts a thorough data investigation across endpoints, quickly identifying infected devices across the network and defining response strategies for detected threats.

The system supports multi-faceted response measures for malicious files/processes, including permission restriction, isolation, deletion, device shutdown, and network blocking. By consolidating single-response actions into global policies, Leagsoft EDR strengthens the security baseline to continuously intercept threats.

5.4 In-depth Threat Investigation

In an Endpoint Detection and Response (EDR) system, continuous monitoring and analysis are critical processes. External threat attacks are unpredictable and constantly evolving, and only by conducting a comprehensive trace analysis of past attack events can weaknesses in the security framework be identified and improved to better defend against future attacks.

Leagsoft EDR supports correlation queries and evidence retention based on various pieces of information, such as domain names, MD5 hashes, processes, ports, and IPs. It enables detailed tracking of file origins, process startup commands, parent-child process relationships, system usernames, helper IDs, system services, startup types,

process access to domains and ports, DNS resolution, and more. This provides a better understanding of endpoint activities, offering contextual information and details about attacks.

Additionally, the system allows unified viewing and modification of policies, patch fixes, plugins, network settings, processes, software, audit information, operating system accounts, services, and system events on specified endpoints. This capability provides users with the necessary evidence and basis for attack tracing and forensics.

5.5 Endpoint Threat Response

When malicious files appear within an enterprise's intranet, they are often challenging to eradicate due to cross-infection and other factors fully. Traditional antivirus software addresses these threats by performing full network-wide scans and removals, but this approach is time-consuming and can disrupt normal business operations, especially in large networks with thousands of endpoints, making simultaneous network-wide eradication difficult.

Leagsoft EDR enables comprehensive tracing of malicious files/processes detected on individual endpoints within the intranet. Using custom global searches or YARA and Braise syntax, the system conducts thorough investigations across endpoints to swiftly identify infected devices across the network and define response strategies for detected threats.

The system supports a range of response measures for malicious files/processes, including permission restriction, isolation, deletion, device shutdown, and network blocking. By standardizing individual responses into global policies, Leagsoft EDR raises the security baseline, providing continuous threat interception.

5.6 Integration with Security Products

Supports deep integration with other endpoint security products from Leagsoft, such as network access control and endpoint security management. It supports interfaces like Syslog and Webservice to notify third-party vendor analysis platforms of raw data and analysis results and provides an OPEN API interface for integration with third-party security analysis vendors for coordinated response and investigation. It offers multi-faceted response measures for malicious files/processes, including permission restriction, isolation, deletion, device shutdown, and network blocking.

6. Product Advantages

6.1 Comprehensive Data Collection and Monitoring

Leagsoft offers a robust terminal security monitoring solution, continuously collecting, monitoring, and analyzing endpoint security data to significantly enhance threat detection capabilities. Currently, it supports the collection of over 18 categories and 336 sub-categories, covering a wide range of data points associated with common attack techniques.

6.2 High-Speed Data Engine

Leveraging endpoint security system storage data, Leagsoft has developed the AcutaDB cache service—a specialized data engine that omits seldom-used traditional database functions, such as transactions, to optimize data access speed. This approach enhances data retrieval speeds by over ten times compared to conventional databases, supports fast storage/read operations for billions of records, and is compatible with cluster deployments.

6.3 Customizable Expert Rule Analysis

With multi-syntax support for detection models, the solution enables customizable detection across various dimensions (static/dynamic). It supports complex expert rule definitions, integration of open-source rules, and reuse of customer-specific rule libraries.

6.4 Advanced Investigation and Analysis Platform

The platform facilitates comprehensive threat tracking, analysis, and investigation. An in-depth examination of threat events and associated endpoint context helps identify the network kill chain and reconstruct event sequences.

6.5 Automated Threat Response

For advanced threats, the solution provides tailored response strategies, including isolation, termination, and forensic capabilities, to quickly halt threat progression. This automation enhances the security operations team's responsiveness and overall threat management efficiency.

7. Product Value

7.1 From Passive to Proactive Protection

Traditional endpoint security products, such as EPP, NAC, and AV, rely on pre-set security policies to counter known security threats or apply baseline settings. Leagsoft EDR employs an adaptive security architecture that continuously monitors endpoint security status and detects suspicious behavior in real time, enabling it to quickly identify threats. By conducting a thorough traceability analysis of detected attack events, it uncovers gaps in the security framework, further improving the system to prevent future attacks.

7.2 From Broad Detection to Precision

Through real-time monitoring of endpoint activities, Leagsoft UniEDR records all endpoint actions while leveraging security clues, attack signatures, and big data analytics to identify unknown risks within the enterprise network. It provides comprehensive context and details for in-depth threat assessment, identifying threat samples and impacts. UniEDR also supports custom security alert models tailored to business needs, creating a multi-dimensional, multi-layered deep detection system for files, processes, host access, and business relationships. This enables continuous monitoring of intrusions, real-time intrusion detection, and rapid response, issuing millisecond-level alerts upon detecting anomalies.

7.3 From Slow to Fast Response

With EDR's detection and response capabilities, combined with a well-designed security response process, security operations teams are guided to search for and extract additional information within the network, investigating the true intent of advanced threat penetration. This enables security personnel to quickly define scope, assess impact, and mitigate losses promptly, enhancing emergency response efficiency.

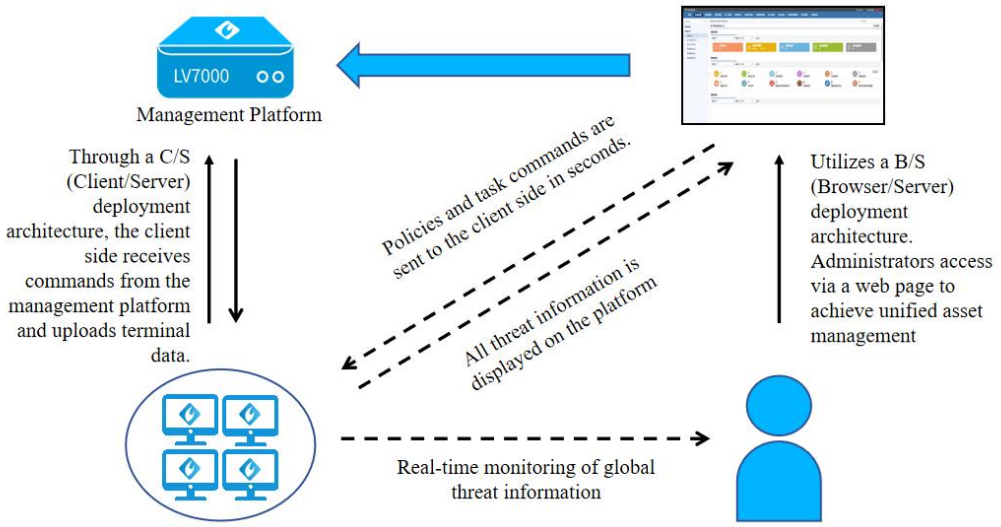
7.4 From Isolated to Integrated Collaboration

Leagsoft UniEDR integrates seamlessly with EPP platforms, enabling unified management through a single platform and client, reducing endpoint resource usage and minimizing user resistance. Equipped with various data transmission interfaces, including Syslog, Webserver, and Web API, the platform can integrate with an organization’s internal threat detection and response framework.

8. Deployment Methods

Leagsoft EDR is adaptable to various network environments, including the internet, isolated networks, cloud, and virtualization environments. It supports multiple deployment methods across different application scenarios, including integrated, distributed and hierarchical deployment. It also allows a single management center to centrally and uniformly manage mixed deployments across physical and virtual environments

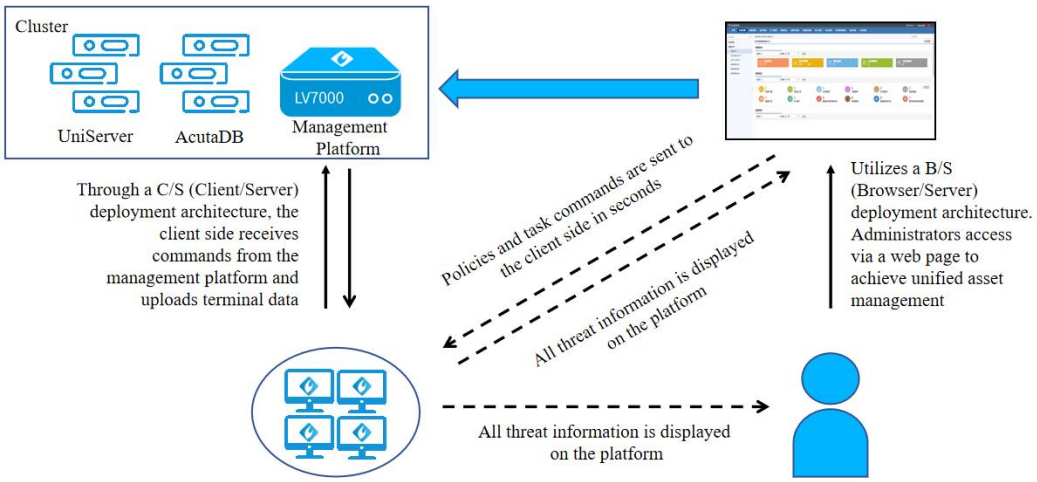
8.1 Standalone Deployment



Leagsoft EDR Standalone Deployment Diagram

8.2 Distributed Deployment

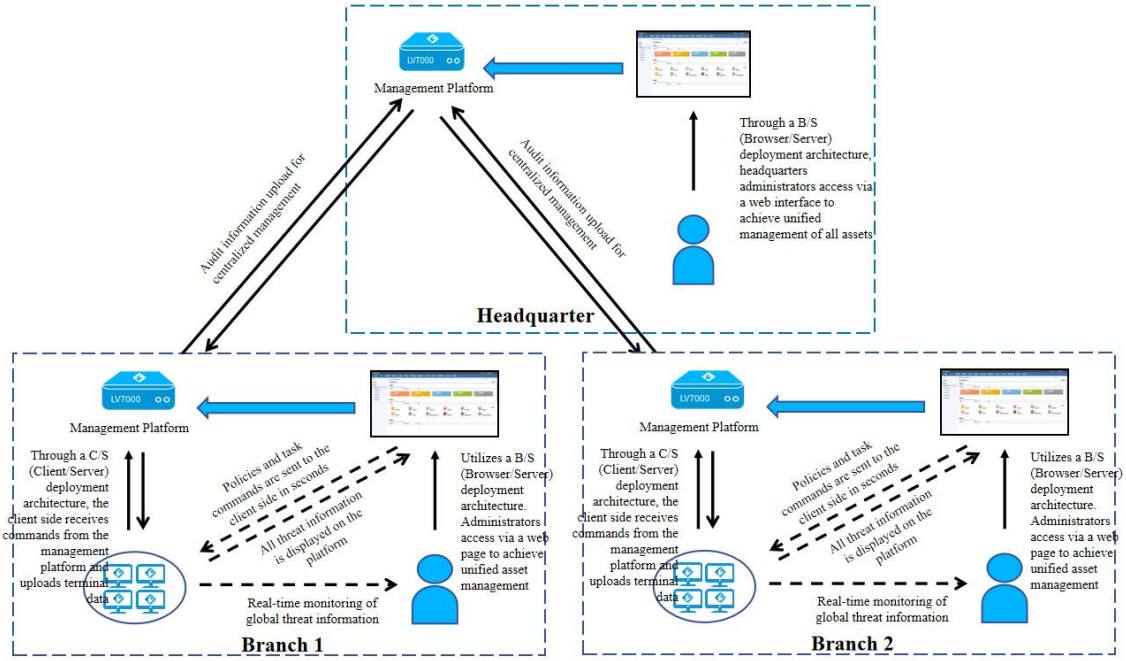
When the number of endpoints exceeds a certain scale, some modules in standalone deployment may experience performance bottlenecks. In this case, it is necessary to deploy certain modules separately, i.e., through distributed deployment.



Leagsoft EDR Distributed Deployment Diagram

8.3 Hierarchical Deployment

"Hierarchical Deployment" primarily involves the division of administrator permissions, data synchronization between levels, and tiered management.



Leagsoft EDR Hierarchical Deployment Diagram

9. Application Scenarios

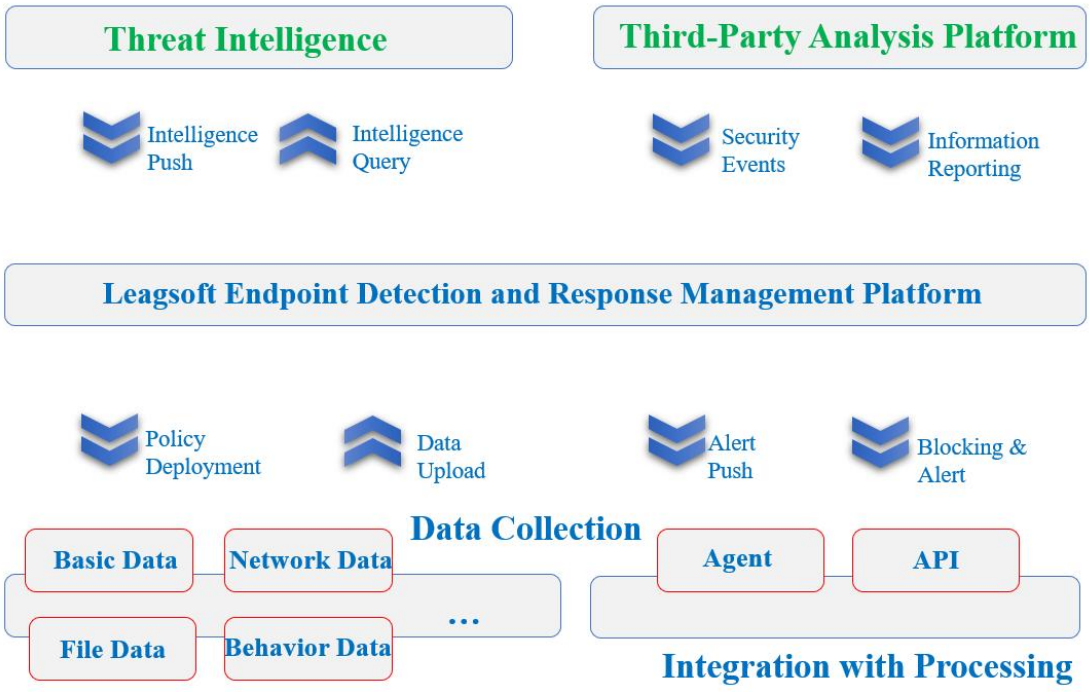
9.1 Scenario 1: Network-Cloud Integrated Threat Response

When a suspicious behavior is detected, it must undergo multi-dimensional verification and interpretation before being definitively identified as an attack, to avoid false positives and missed detections. The UniEDR system from Leagsoft can provide comprehensive endpoint data collection for analysis and investigation on an integrated threat detection platform. This allows for tracing the source of threats, identifying the propagation paths and attack methods, assessing the impact, confirming the affected endpoints, and implementing targeted system-hardening measures and responses.

For instance, when an administrator receives a security incident report from a third-party analysis platform or an IOC (Indicators of Compromise) alert from a

higher authority—such as a sample MD5 hash or a C2 (Command and Control) address—Leagsoft's EDR system can quickly confirm the circulation status of the sample across the entire network using its security investigation features. It can also identify the origin of the malicious file and reconstruct the entire attack process.

Moreover, for identified abnormal endpoints and malicious files, the EDR system provides corresponding isolation functionalities, such as host isolation, process isolation, and file isolation.



9.2 Scenario 2: Proactive Analysis of Unknown Threats

Selecting Investigation Content and Targets

The first step for analysts is to formulate an investigation theme, which can be derived from the following sources:

Threat incidents detected by the system, such as IOCs (Indicators of Compromise) disclosed in public internet security events, including sample MD5 hashes, C2 addresses, or other characteristic information.

Common attack methods used by attackers at the endpoint level, such as brute-force password attacks, phishing emails, and vulnerability exploits during the intrusion phase.

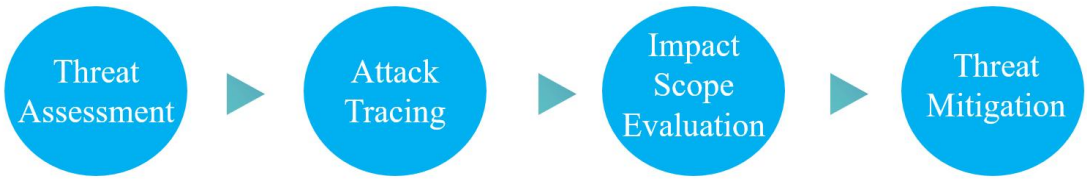
Detection conditions and thresholds set by security operations personnel based on the organization's specific security environment.

Security analysts, considering their organization's environment and the types of attacks faced, can establish initial search criteria to define the investigation scope and identify a suitable starting point. For instance, when addressing external threats like brute-force password attacks, analysts can narrow down the investigation by searching through user login records or combining conditions related to connection requests on specified network ports.

Aggregated Data Investigation and Analysis:

After defining the investigation theme, threat tracking will provide search results related to the theme from a logging perspective. To enhance the efficiency of log analysis, analysts need to extract information quickly from the data using different aggregation dimensions according to the current investigation stage.

The process for handling unknown threats can be summarized into four main steps: **Threat Assessment**, **Attack Tracing**, **Impact Scope Evaluation**, and **Threat Mitigation**.



Threat Assessment:
When abnormal behavior is detected on certain endpoints, it is essential to combine the organization's internal security context, policies, and a large volume of multi-dimensional endpoint data to determine the nature of the threat. This helps analysts verify whether an endpoint has been compromised. For instance, analysts might aggregate PowerShell process “run command” data to retrieve parameters used during remote login and check for any anomalies.

Attack Tracing:
Once signs of an unknown threat are identified, a deeper analysis is required to uncover the attack methods used, the source of the delivery, and the behavior trail after the connection. For example, analysts need to determine which channel was used to successfully infiltrate the network, which devices were infected post-intrusion, and what techniques were used for lateral movement. The process may include identifying sub-processes called during the attack, commands executed, external network connections established, and any backdoor programs left behind.

Impact Scope Evaluation:

Once the attack methods and pathways are clearly traced, analysts can use the corresponding behavior characteristics to search for other devices with similar or related attributes, thereby evaluating the asset coverage and impact range of the current threat stage.

Threat Mitigation:
Based on the attack tracing and impact assessment, the defense strategies and baseline checks can be dynamically adjusted. This includes blocking the identified attack paths, reinforcing the system hardening measures, and implementing responsive countermeasures to mitigate the threat.

9.3 Scenario 3: Compromised Endpoint Investigation and Forensics

When an endpoint is flagged for investigation or detected by an EDR alert as compromised (e.g., infected with ransomware), and there is a concern that the threat could spread to other endpoints, the first step in an emergency response is to **isolate** the compromised endpoint. This containment prevents the threat from expanding within the internal network, buying time for final resolution.

For such scenarios, EDR provides an endpoint isolation function, enabling **"endpoint isolation"** for a single compromised device. Once confirmed, this isolation restricts the endpoint's communication solely to the control console, ensuring it can still receive policy and task updates but is cut off from other network communications. This allows for in-depth forensic analysis, helping analysts gain a comprehensive view of the attack process and understand the technical tactics and methods used at each attack stage.

Finally, by thoroughly analyzing the attack techniques and methods identified at each stage, security gaps in the system can be uncovered. This information is then used to develop ongoing containment strategies to prevent similar attacks in the future.